SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Program Strategy & Operations > Emerging Issues >

Is it Time for a Corporate Security Maturity Assessment?

By George Campbell, Emeritus Faculty, Security Executive Council

Over the past few years, the Security Executive Council (SEC) has been examining a variety of applications to assist in the implementation of operational excellence (OpEx) in security program management. In this paper, we address the potential benefits of creating a Capability Maturity Model (CMM) as an enabling process in OpEx. As an OpEx enabler, business process maturity assessments have been around for a number of years[1] in support of process transformation efforts. As tools, they are useful models because they seek to provide straightforward results that are simple to understand and direct in terms of where to focus on measurable improvements.

The Capability Maturity Model (CMM) was originally developed by DoD as a tool for objectively assessing the ability of government contractors' processes for implementing contracted software projects. Though the model comes from the field of software development, it is also used to aid in business process improvement generally, and has also been used extensively worldwide in government offices, commerce, and industry. There are a variety of maturity models at work in the business literature depending on how granular or process-directed one desires to be. This paper seeks to employ the general framework that may be found across the various models and apply it specifically to the core processes that comprise the elements of a corporate security program.

A CMM for Corporate Security?

Maturity models typically (and very correctly) focus on individual programs like IT security, which is totally appropriate for drilling down on a more directed set of capabilities. But how to connect the dots across Security's big picture? Quite simply, this focus can capture (and force) a more inclusive set of programs and services that collectively support the CSO's *more integrated* risk management mission. This is a

[1] See The Process Audit, Harvard Business Review, April 2007 and the Capabilities Maturity Model, Carnegie Mellon Software Engineering Institute, 2007 for a complete discussion of these models

critical perspective for a security executive and the assessment result can enable a highly informative communication with senior management.

Consider the interdependencies among these various programs. Investigations support an ethical business environment. Physical security provides an envelope around IT security and multiple elements of access control, personnel, space and point protection. Contingency planning is critical to supply chain and business process resilience. Risk assessment is the key enabler for setting protection priorities and informing an all-hazards risk program. When we focus exclusively on any one of these, we can miss how a specific strength or weakness in process maturity may contribute or detracts to the objective of an integrated protection strategy. Of specific relevance to operational excellence, CMMs focus on best practices drives a more critical assessment of those inter-dependent processes that can be lost in a more limited view.

With that brief introduction, let's examine CMM's value to a proactive security strategy.

How Can a CMM Add Value to Corporate Security?

A maturity model provides several benefits for a security executive seeking to build a plan for organizational development:

1) It's an easy and team-building place to start.
2) It benefits from prior experiences.
3) It provides for a common language and shared vision.
4) It enables a framework for prioritizing actions.

5) Perhaps most importantly, CMM provides a way to define what improvement means for your organization.

Here again is the relevance to operational excellence. Capability is about proficiency, competence and the confirmed skills to execute essential tasks. Maturity is about reliability and indicates levels of acceptance and established practice. A mature process has proven practices that have consistently delivered valued results to the organization. Understanding the current levels of proficiency and acceptance of security processes within an organization should be essential steps in building and maintaining a Corporate Security business plan.

How might a set of industry-accepted measures around the competency and reliability of components of a Security program serve to define excellence and value? A CMM focused on a selective inventory of security principles and standards can provide the Chief Security Officer, his/her team and their stakeholders with actionable status of protection program content and management capabilities as well as factors that directly influence and support a multi-faceted corporate security program.

A high value return is provided by using a CMM for business management to understand the scope and purpose of various elements of the security program. For Security management, the gap analysis process establishes priorities and facilitates connecting the dots on targets for improvement aligned with a relevant set of rank-ordered measures and metrics[2] to anchor and track status and progress of directed improvements to individual elements.

A CMM Facilitates Risk Assessments

The CMM process can be a precursor for more detailed risk assessments. Risk assessment is acknowledged as a core process that seeks to identify the vulnerabilities in the organization's established protection capabilities and then provide support for a determination of where investments will be made in mitigating identified gaps or accepting the consequences of an event. There is an essential linkage between security process maturity and the fundamental obligation of a security executive to understand and anticipate the depth and breadth of risk to the enterprise. Unfortunately, what we often see in these assessment processes is a lack of scope: a periodic, check-the-box / fill-in-the-blank exercise that fails to extend the assessment into the competence of related security-dependent capabilities. CMM has the ability to push these enterprise protection elements for a more accurate fix on their respective competence and reliability.

A common corporate security organizational model is a vertical array of functionally specialized[3] and vertically-oriented silos. Their respective programs are resourced, delivered and measured within the confines of assigned organizational units and managers. From a typical service delivery model, accountability for results may be achieved (or not) within the four walls of the silo. CMM's value is in its focus of connecting the dots *horizontally* across these silos and probe where interdependencies and

[2] The output of a maturity assessment exercise provides some very solid and actionable metrics for support to improvement initiatives and management reporting. Consider the opportunity of moving a core capability from a basic to competent and then to measurably effective and then demonstrating how this incremental improvement has yielded results for the business.

[3] Physical security, investigations, business continuity, safety, information security, etc.

inefficiencies may present opportunities for improved protection, lower cost and higher value for the customer.

CMM and Security's Stakeholders

Senior executive commitment and a supportive corporate culture are the cornerstones of an effective enterprise security program. As Security executives, we often fail to educate our stakeholders on what an effective risk and customer-responsive security program should look like. A well-documented and maintained maturity assessment will have a history of executive engagement in program content and effectiveness. But, it's also true that Security has to compete for management's engagement especially where the competition is fierce, strategy is stressed, and the flagpole is far over the horizon. We often see these conditions driving top-down, cost reduction initiatives and deeper dives into basis of estimate (BoE) and reengineering. The CMM's results can directly support and provide useful pointers in these more in-depth process reviews.

What Should the CMM Process Entail?

A critical first step is a planning session to review the various line items and their measurement options, a thorough review of the terminology in the table, determine where preparatory documentation review is required for informing a ranking decision and to identify gaps in data required for individual capability assessment. The review team should ideally consist of senior members of each security function being included in the review. This is particularly important where site security operations are being included since local knowledge is critical to accuracy. And it may seem obvious – but objectivity is critical to the results.

Where Do We Go from Here?

Creating a CMM specific to Corporate Security will not be a trivial process. Each business or organization has a different suite of security programs and services. Definitions used in a CMM assessment will need to be generalized but what about the specific cultural, legal, business process and risk management framework within the user's organization? Do we assess the entire security function or by the processes in individual programs or services? And what do we do with the results? It's an all too common and noteworthy fact that program performance assessment processes often fail to provide necessary and actionable descriptors of quality and measurable capability when a notable event advertises its' failures rather than directing its' benefits.

The SEC is actively exploring these questions and has a start on a few versions of a CMM specific to Corporate Security. For those interested in this topic, please contact us so we can broaden this discussion.

Visit the Security Executive Council web site to view more resources in the Security Program Strategy & Operations > Emerging Issues > series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

